

FILED

APR 12 2023

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

CLERK, U.S. DISTRICT COURT
NORTH DISTRICT OF CALIFORNIA

DAVID ANGEL SIFUENTES III,
Plaintiff,

CASE NO.
HONORABLE:

CV 23-1758

V.

TWITTER INC,

Defendant.

DEMAND FOR JURY TRIAL

**COMPLAINT WITH MEMORANDUM OF LAW AND DEMAND FOR
JURY TRIAL**

Now comes, the Plaintiff David Angel Sifuentes III, In Pro Se and submits complaint with memorandum of law and demand for jury trial, seeking relief for identity, personal information, (data) being exposed and stolen from a data breach from Twitter Inc., which Sifuentes has Constitutional Standing under the United States Constitution Article III "imminent" risk of identity theft or fraud" to bring this complaint. *See In re Zappos.com, Inc.*, 884 F.3d 893 (9th Cir. 2018), *Galaria v. Nationwide Mutual Insurance Co. No.*, 663 F.App'x 384 (6th Cir. 2016), invasion of privacy by public disclosure of private facts, negligence, negligence per se, implied right of private action under Federal Trade Commission 15 U.S.C. § 45(a)(1), breach of fiduciary duty, unjust enrichment, breach of implied contract, negligent and or intentional infliction of emotional distress, conversion (use of information without permission) breach of bailment, failure to promptly notify of the breach and provide security measures and protection to Sifuentes for the breach, and risk of future injury, California Data Breach law Cal. Civ. Code § 1798.82, also the Michigan Consumers Protection Act. Sifuentes is seeking damages of \$375,000.00 and punitive damages of \$350,000,000.00 for a total of \$350,375,000.

Sifuentes ask this Court to liberally construe his pleadings, legal documents, arguments and not fault him for not citing are applying the correct case law, statute and applicable laws under *Haines v. Kerner*, 404 U.S. 519 (1972). Pro se litigants can be excused from full compliance with technical procedural rule, provided there is substantial compliance. *Norefleet v. Walker*, 684 F.3d 688 (7th Cir. 2012). Court and staff have a special responsibility to scrutinize carefully pro se

complaints. *Chapman v. Kleindienst*, 507 F.2d 1246, 1253 (7th Cir. 1974) (district court has responsibility for finding hidden jury demands in the middle of complaints).). A court must accept all allegations of well-plead factual allegations as true, *League Am. Citizens v. Bredesen*, 500 F.3d 523, 527 (6th Cir. 2007), and factual allegations alone is what matters. *Albert v. Carovano*, 851 F.2d 561, 571 n.3 (2nd Cir. 1988). Please note that Sifuentes relies on his exhibits he filed on November 28, 2022 with his original complaint in support of this amended complaint.

Jurisdiction

This court has **both personal and diversity jurisdiction** under this complaint, This court has jurisdiction diversity Jurisdiction as Twitter Inc. is a cooperation head quartered in San Francisco, California, David Angel Sifuentes III is a citizen of Michigan, and therefore the parties are different citizens and this court has jurisdiction of all civil matters as the damages are more than \$75,000 28 U.S.C. § 1332. Sifuentes is seeking damages of \$375,000.00 and punitive damages of \$350,000,000.00, which can also be added for jurisdictional purposes. *Hayes v. Equitable Energy Res. Co.*, 226 F3d 560 (6th Cir. 2001). This Court also has supplemental jurisdiction under 28 U.S.C. § 1367 of Sifuentes state law claims.

“Standard of Review” Article III standing and jurisdiction “personal injury”

Article III. Section 2 of the United States Constitution:

The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority;--to all Cases affecting Ambassadors, other public Ministers and Consuls;--to all Cases of admiralty and maritime Jurisdiction:--to Controversies to which the United States shall be a Party;--to Controversies between two or more States;-- between a State and Citizens of another State;-- between Citizens of the same State claiming Lands under Grants of different States, and between a State, or the Citizens thereof, and foreign States, Citizens or Subjects.

Article III confines the federal judicial power to the resolution of “Cases” and “Controversies” in which a plaintiff has a ‘personal stake. “To have Article III standing to sue in federal court, a plaintiff must show, among other things, that the plaintiff suffered concrete injury in fact. Central to assessing concreteness is whether the asserted harm has “close relationship” to harm

“traditionally” recognized as providing a basis for a lawsuit in American courts. That inquiry asks whether plaintiffs have identified a close historical or common-law analogue for their asserted injury. Physical or monetary harms readily qualify as concrete injuries under Article III, and various intangible harms-like reputational harms-can also be concrete. *Transunion LLC v. Ramirez*, 141 S.Ct. 2190, 2198 (2021).

Federal courts have Article III standing and jurisdiction and Sifuentes has standing of the United States Constitution in this court to his data breach complaint. *See In re Zappos.com, Inc.*, 884 F.3d 893 (9th Cir. 2018), *Galaria v. Nationwide Mutual Insurance Co. No.*, 663 F.App’x 384 (6th Cir. 2016). The United States Supreme Court has “found standing based on a ‘substantial risk’ that the harm will occur even if not literally certain the harms will come about. *Galaria*, *supra* citing (*Clapper v. Amnsesty Int’l USA*, 133 S.Ct. 1138, 1150 n.5).

Sifuentes asserts that this Court does have proper jurisdiction under Article III for his data breach claim personal injury theft of his identity. The Sixth Circuit has found that Plaintiff’s allegations were sufficient to establish Article III standing at the pleading stage of the litigation though allegations of actual fraud and identity theft were absent: “Plaintiffs allege that the theft of their personal data places them at a continuing, increased risk of fraud and identity theft beyond the speculative allegations of ‘possible future injury’ or ‘objectively reasonable likelihood’ of injury that the Supreme Court has explained are insufficient.” *Id.* at *9 (*quoting Clapper*, 133 S.Ct. at 1147-48).

Timing

Sifuentes claims are timely under “**common law and California delayed discovery rule**”. *Cada v. Baxter Healthcare Corp.*, 920 F.2d 446, 450 (7th Cir. 1990); *California Sansome Co. v. U.S. Gypsum*, 55 F.3d 1402 (9th Cir. 1995). Also under Michigan, law MCL 600.5805. Although the data breach occurred in 2021, Sifuentes took reasonable steps of investigating the matter once he was put on notice of the and learned of the severability of the breach such as reported by the November 25, 2022 article, and around 2023 by way of data breach monitoring services such as FireFox. Also discovery of fraud is applicable in this matter, *Merck & co. v. Reynolds*, 559 U.S. 633, 644 (2010): *Cf. Rotkiske v. Klemm*, 140 S.Ct. 355 (2019), where Twitter took no action and covered up the breach, no notification was ever sent to Sifuentes to

notify him of the breach. Further Twitter was supposed to inform Sifuentes that his personal identity and information was comprised by the 2021 data breach and never did. Further equitable tolling is equitable to all of Sifuentes claims as he has been exercising due diligence in the investigation of his claims and still suffers harm of the breach where he constantly gets hacked and accounts comprised also bank accounts he did not authorize opened under his name, such as Bank of America.

Facts

On or around January 2023 Sifuentes obtained a report from FireFox (Exhibit A, Firefox Report) See also (Exhibit B, What Twitter's 200 Million-User Email Leak Actually Means) informing him that his data personal information was comprised from Twitter Inc. on or around January 1, 2021 Twitter Inc., which was placed on Firefox data base on January 5, 2023. Sifuentes did not contact Twitter about the breach. Sifuentes has had a Twitter account for sometime since around 2011 along around the same time he had an opened a Facebook account. Twitter failed to secure and protect through careless security and negligence personal information concerning Sifuentes personal information such as the email address he had on file davidsifuentes61@yahoo.com and password which he used for his banking accounts, and other online and social media accounts also linked to his home address and other personal facts, such as Facebook account that contains photos and personal facts of Sifuentes and his family. Further facts may be presented in this pleading. Sifuentes never received any notification of the breach from Twitter. The personal information stolen is currently on the "dark web" and been offered for sale. See (Exhibit C, Twitter Data Breach article, pages 1-3), also according to a Experian dark web scan Sifuentes personal information such as emails and passwords which he used for numerous accounts, the same one used in Twitter Inc., which is "fairly traceable" to the breach Twitter such as his email and password he has been using.

Judicial Notice

Pursuant to Fed. R. Evid. 201(c)(2), the Court “must take judicial notice if a party requests it and the court is supplied with the necessary information.” Types of facts that may be judicially noticed include those that “can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned.” Fed.R.Evid. 201(b)(2). This includes materials that are in the public record. *New England Health Care Employees Pension Fund v. Ernst & Young, LLP*, 336 F.3d 495, 501 (6th Cir. 2003) (“A court that is ruling on Rule 12(b) motion may consider materials in addition to the complaint if such materials are public records or are otherwise appropriate for the taking of judicial notice.”); *Rodic v. Thistledown Racing Club, Inc.*, 615 F.3d 736, 738 (6th Cir. 1980) (“Federal courts may take judicial notice of proceedings in other courts of record.”). Sifuentes ask that this Court take judicial notice of Exhibits A-C, and also the following articles discussed on the effects and worth of data.

The effects and worth of data.

Sifuentes ask that this Honorable Court take judicial notice of the following public online articles in support of his complaint. Data personal identifier information (PII) is very valuable and priceless as there is unlimited potential for cybercriminal’s to do harm. PII is valuable property. See Articles online Marc Van Lieshout, *The Value of Personal Data* at p. 4, 457 *IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY* 26 (MAY 10, 2015), available at https://researchgate.net/publication/283668023_The_Value_of_Personal_Data 9”The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible[.]” (last visited March 11, 2023).

Companies such as Twitter profit from data used from Twitter. Firms are able to attain significant market valuations by employing business models predicated on the successful use or personal data within the existing regulatory and legal frameworks. See *Exploring the Economics of Personal Data: A Survey of methodologies for Measuring Monetary Value*, *OECD Digital Economic Papers* no. 220 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last visited April 4, 2023). See *U.S. Firms to Spend Nearly \$19.2 billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (De. 5, 2018), <https://www.iab.com/news/2018-state-of-data-report/> (last visited April 4, 2023).

PII can be sold from anywhere from \$40 to \$200, and bank details have a price range of \$50 to \$200. Anita George, *Your personal data is for sale on the dark web*. Here's how much it costs, Digital Trends (Oct. 16, 2019), <https://www.digitaltrends.com/computing/peronsal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited March 11, 2023). Criminals can also purchase entire data breaches from \$900 to \$4,500. In the Dark, VPNOverview.com, 2019, <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed on April 4, 2023). Experian has found that stolen debit and credit cards details can sell for \$5 to \$110 on the dark web. Brian Stack, *Here's How Much Your Personal Information is Selling fro on the Dark Web*, Experian (Dec. 6, 2017), <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited April 4, 2023).

Twitter collects and sells information concerning consumers and there habits, as consumers place a high value on the privacy of that data. There has been research that sheds light on how much consumers value their data privacy-and the amount is considerable. Indeed, studies confirm that “when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites. Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) *INFORMATION SYSTEMS RESEARCH* 254 (June 2011), <https://www.jstor.org/stable/23015560?seq=1> (last visited April 4, 2023). Cyberattacks have become so frequent that the U.S. Secret Service and FBI have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals...because they often have a lesser IT defenses and a high incentive to regain access to their data quickly. Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, *LAW360* (Nov. 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware> (last visited April 4, 2023).

Data is very valuable and criminals have a need to use that property that is individuals PII.

Complaint and memorandum

i. Article III “concrete injury” “imminent” risk of identity theft or fraud”.

On or about January 2023 Sifuentes found that he was a victim of a data breach from Twitter from Firefox (See Exhibit “A”) notifying him that his data PII personal information had been compromised Twitter never informed Sifuentes of this breach. A data breach victim may seek relief in Federal Court when a company has failed to protect the data of its customers. See *Galaria v. Nationwide Mutual Insurance Co.*, 663 F.App’x 384 (6th Cir. 2016). This includes heightened risk of future injury, *In re U.S. Office of Personnel Management Data*, 928 F.3d 42 (D.C. Cir. 2019). A litigant need not provide proof of monetary damage to bring a claim of data breach in Federal Court. A plaintiff threatened with future injury has standing to sue “if the threatened injury is ‘certainly impending,’ or the risk that the harm will occur. See *In re Zappos.com, Inc.*, 884 F.3d 893 (9th Cir. 2018). A litigant need only provide *concrete proof* that his personal information had been comprised by the breach. See *Transunion LLC v. Ramirez*, 141 S.Ct. 2190 (2021).

Sifuentes has show in injury in fact and concrete injury of the data breach where his identity has been stolen that is his personal data and information from Twitter which includes his user name, passwords, email, and his name social media profiles, such information can and has been comprised which leads to hackers using the data to commit crime are assume the Identity of Sifuentes that is identity theft a concrete injury, *Transunion LLC, v. Ramirez*, 141 S.Ct. 2190 (2021); *Galaria v. Nationwide Mutual Insurance Co. No.*, 663 F.App’x 384 (6th Cir. 2016); *Clemens v. ExecuPharm Inc.*, 48 F.4th 146 (3rd Cir. 2022):

Article III standing requires a plaintiff to demonstrate.” (1) that he or she suffered an injury in fact that is concrete, particularized, and actual or imminent, (2) that the injury was caused by the defendant, and (3) that the injury would likely be redressed by the requested judicial relief. this court does not have jurisdiction and his state law claims should proceed in federal court.Id., citing cases.

Here the data breach occurred that is theft of Sifuentes identity, two the injury-in-fact is actual or imminent as the data from Twitter that is email, passwords, social media personal facts still and endure the kind of future harm that qualifies as ‘imminent.” *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 152 (3rd Cir. 2022). The data could be used to open bank accounts and other accounts and commit crime that is cybercrimes with it.

ii. Invasion of privacy by public disclosure of private facts, intentionally, willfully, recklessly, and negligently failed to protect data.

Sifuentes has suffered invasion of privacy by public disclosure of private facts where his personal information PII data has been exposed and stolen and taken without him knowing and without permission his personal property being his data from Twitter. Twitter ‘intentionally, willfully, recklessly, and negligently’ failed to take sufficient measures to safeguard the data. Twitter did not follow the guidelines for a data breach as required by the Federal Trade Commission. Sifuentes has indeed suffered concrete injury in fact, due to the exposure of his personal information. *TransUnion v. Ramirez*, 141 S.Ct. 2190 (2021).

iii. Bailment

Twitter has violated bailment, failure to promptly notify of the breach and provide security measures and protection to Sifuentes for the breach. Here Sifuentes delivered valuable digital information that is his property and trusted that information would be secured to Twitter. The goods or Twitters collection of data and information. Without the information Twitter would not be in business because they use data to make profit, See Article *U.S. Firms to Spend Nearly \$19.2 Billion on Third-Party Audience data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), <https://www.iab.com/news/2018-state-of-data-report/> (last visited March 18, 2023).

As Blacks law dictionary 6th edition defines Bailment as:

A delivery of goods or personal property, by one person (bailor) to another (bailee), in trust for the execution of a special object upon or in relation to such goods, beneficial either to the bailor or bailee or both, and upon a contract, express or implied, to perform the trust and carry out such object, and thereupon either to redeliver the goods to the bailor or otherwise dispose of the same in conformity with the purpose of the trust.

The bailee is responsible for exercising due care toward the goods....
p. 141-142.

Definitely data is goods and valuable and worth a lot of money to data thieves See Article *Brian Stack, Here's How Much Your Personal Information Is Selling for in the Dark Web*, Experian (Dec. 6, 2017), <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited March 18, 2023).

iv. Negligence

Twitter owed a duty to Sifuentes to protect his data on Twitter to exercise reasonable care in safeguarding and protecting his PII in its possession, custody, or control. Twitter knew, or should have known, the risks of collecting and storing Sifuentes and other users' personal tweets and data, and the importance of maintaining secure systems. Twitter knew, or should have known, of the vast uptick in data breaches in recent years. Twitter had a duty to protect the PII of Sifuentes.

Given the nature of Twitter's business, the sensitivity and value of the PII it maintains, and the resources at its disposal, Twitter should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring, which Twitter had a duty to prevent.

Twitter breached these duties by failing to exercise reasonable care in safeguarding and protecting Sifuentes's PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to—including Sifuentes' PII.

v. Negligence Per Se

Twitter's duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair... practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Twitter, of failing to employ reasonable measures to protect and secure PII. Sifuentes seeks an implied right of private action under 15 U.S.C. § 45(a)(1). The statute remains silent and has no language prohibiting an implied right of private action.

Twitter violated Section 5 of the FTCA by failing to use reasonable measures to protect Sifuentes and all other users affected by the breach, and not complying with applicable industry standards. Twitter's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of data breach involving PII including, specifically, the substantial damages that would result to Sifuentes. Twitter's violations of Section 5 of the FTCA constitute negligence per se.

vi. Breach of fiduciary duty

Sifuentes and users either directly or indirectly gave Twitter their PII in confidence, believing that Twitter would protect that information. Sifuentes and users would not have provided Twitter with this information had they known it would not be adequately protected. Twitter's acceptance and storage of Sifuentes's created a fiduciary relationship between Twitter and Sifuentes. In light of this relationship, Twitter must act primarily for the benefit of its customers, which includes safeguarding and protecting Sifuentes's PII.

Twitter has a fiduciary duty to act for the benefit of Sifuentes and upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Sifuentes's and users PII, failing to comply with the data security guidelines set forth by Section 5 of the FTCA, and otherwise failing to safeguard the PII it collected and collects.

vii. Unjust Enrichment

Data is a business and Twitter collects a monetary benefit upon users, and selling data. Twitter accepted or had knowledge of the benefits conferred upon it by Sifuentes. Twitter also benefited from the receipt of Sifuentes and Twitter users.

As a result of Twitter's conduct, Sifuentes suffered actual damages in an amount equal to the difference in value between his valuable data used to make profit made with reasonable data privacy and security practices and procedures that Sifuentes and paying Twitter users without reasonable data privacy and security practices and procedures that they received.

viii. Breach of Implied Contract

Twitter required Sifuentes and users to provide, or authorize the transfer of, their PII in order for Twitter to provide services. In exchange, Twitter entered into implied contracts with Sifuentes in which Twitter agreed to comply with its statutory and common law duties to protect Sifuentes's PII and to timely notify him in the event of a data breach.

Sifuentes would not have provided their PII to Twitter had they known that Twitter would not safeguard their PII, as promised, or provide timely notice of a data breach.

ix. Negligent and or intentionally infliction of emotional distress.

Sifuentes is going through negligent and intentional infliction of emotional distress as his personal information has been stolen for nearly two years plenty of time for hackers and cyber criminals to cause harm. It is “fairly traceable” that the stolen data for Twitter may have indeed caused Sifuentes other accounts to be hacked by cyber criminals have had access to Sifuentes accounts such as Spotify, Netflix which hackers from India and even Canada have access his Spotify account and even his PayPal account, which is a bank account. Due to the breach, Sifuentes now wastes his time always switching his password making calls to Banks such as bank of America and wasting time and resources to protect his personal information. This is stressful and Sifuentes is scared as hackers can commit crimes with his personal information and the Spotify account has access to even more personal information of Sifuentes such as his Facebook account, PayPal and credit card information. Sifuentes information is also on the dark web.

x. Risk of future and ongoing injury.

Sifuentes has presented actions which might suffer future concrete injury. *Spokeo, Inc. v. Robins*, 578 U.S. 330 (2016). Here the data breach occurred that is theft of Sifuentes identity, two the injury-in-fact is actual or imminent as the data from Twitter that is email, passwords, social media personal facts still and endure the kind of future harm that qualifies as ‘imminent.’ *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 152 (3rd Cir. 2022). The data could be used to open bank accounts and other accounts and commit crime that is cybercrimes with it. Sifuentes case does raise and Article III standing where his identity has been stolen that is his personal data and information from Twitter which includes his user name, passwords, email, and his name social media profiles, such information can and has been comprised which leads to hackers using the data to commit crime are assume the Identity of Sifuentes that is identity theft a concrete injury, *Transunion LLC, v. Ramirez*, 141 S.Ct. 2190 (2021); *Galaria v. Nationwide Mutual Insurance*

Co. No., 663 F.App'x 384 (6th Cir. 2016); Clemens v. ExecuPharm Inc., 48 F.4th 146 (3rd Cir. 2022).

xi. Conversion

Twitter is in violation of conversion that is unauthorized assumption and exercise of the right of ownership over goods or personal data belonging to Sifuentes. The data breach was an unauthorized act depriving Sifuentes of his personal property that is his PII with Twitter.

This was inconsistent violation of conversion wrongful exercise of Sifuentes personal property that is his PII.

xii. Michigan Consumer protection Act.

Twitter is in violation of the Michigan Consumer Protection Act Mich. Comp. Laws Ann § 445.901 for deceptive practices by covering up the breach and not notifying him of the breach. Also misrepresenting that the goods being data was protected.

Twitter failed to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach.

xiii. California Data Breach law Cal. Civ. Code § 1798.82

Twitter is in violation of the California Data Breach law. As mentioned earlier they did not provide adequate security measures and protect Sifuentes PII.

xiv. Damages

As discussed data is valuable , priceless, and Sifuentes requests for damages is reasonable in this matter as there is unlimited potential for criminals to recycle and continue to use Sifuentes personal data also many other users. Sifuentes is seeking \$375,000.00 for actual damages for injuries caused by both negligent and intentional infliction of emotional distress such as being

very mad, angry, and scared, worried, nervous and has trouble sleeping and scared of what else hackers whole stole his information will do as they keep accessing his accounts and his information is in the dark web., also bank account opened under his name.

Sifuentes seeks \$350,000,000.00 in exemplary, economic and non-economic damages, compensatory and punitive damages injunctive and declaratory relief as this is calculated from the fines and penalties associated from companies concealing data breaches from victims such as the Equifax which settled for \$575,000,000 Capital data breach that settled for \$190 million for failing to take action with data breach protocols.

RELIEF REQUESTED

WHEREFORE, Sifuentes **PRAYS** that this Honorable court grant relief as follows:

Award Sifuentes \$375,000.00 in actual damages for negligent and intentional infliction of ongoing emotional distress for being mad upset and under stress and \$350,000,000.00 in exemplary, compensatory and punitive damages injunctive and declaratory relief, for a total of \$350,375,000 or in the alternative Award \$275,000.00 in actual damages and that Twitter provide Sifuentes with 5 years of LifeLock to help clean and restore Sifuentes identity.

Respectfully submitted,

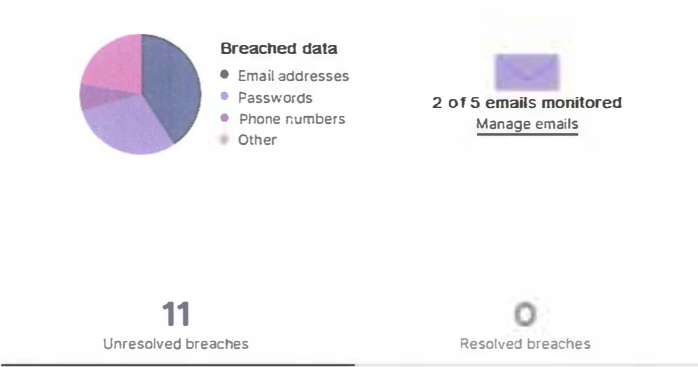
By: 


Plaintiff In Pro Se
David Angel Sifuentes III
439 More St. NE
Grand Rapids, MI 49503
(616)283-5215
davidsifuentes61@yahoo.com

DATED: April 5, 2023

EXHIBIT A

Data breaches for [davidsifuentes61@yahoo.com](#) ▾



COMPANY	BREACHED DATA	DETECTED
 Twitter (200M)	Email addresses	<div>Active</div> 01/05/2023 

On January 1, 2021, Twitter (200M) was breached. Once the breach was discovered and verified, it was added to our database on January 5, 2023. This breach included: Email addresses

Resolve this breach:

1. Protect your email with an email masking service like Firefox Relay.
- This can hide your true email address while forwarding emails to your real inbox.*



EXHIBIT B

LILY HAY NEWMAN SECURITY JAN 6, 2023 9:00 AM

What Twitter's 200 Million-User Email Leak Actually Means

The exposure of hundreds of millions of email addresses puts pseudonymous users of the social network at risk.



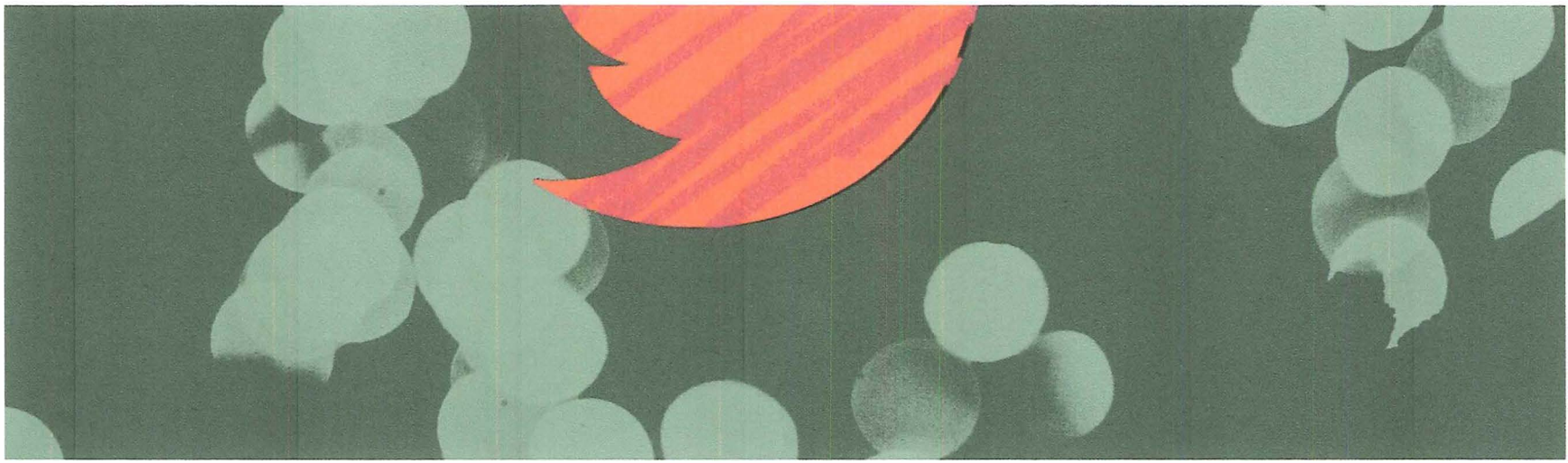


ILLUSTRATION: ROSIE STRUVE; GETTY IMAGES

From June 2021 until January 2022, there was a bug in a Twitter application programming interface, or API, that allowed attackers to submit contact information like email addresses and receive the associated Twitter account, if any, in return. Before it was patched, attackers exploited the flaw to “scrape” data from the social network. And while the bug didn't allow hackers to access passwords or other sensitive information like DMs, it did expose the connection between Twitter accounts, which are often pseudonymous, and the email addresses and phone numbers linked to them, potentially identifying users.

While it was live, the vulnerability was seemingly exploited by multiple actors to build different

collections of data. One that has been circulating in criminal forums since the summer included the email addresses and phone numbers of about 5.4 million Twitter users. The massive, newly surfaced trove seems to only contain email addresses. However, widespread circulation of the data creates the risk that it will fuel phishing attacks, identity theft attempts, and other individual targeting.

Twitter did not reply to WIRED's requests for comment. The company wrote about the API vulnerability in an August disclosure: "When we learned about this, we immediately investigated and fixed it. At that time, we had no evidence to suggest someone had taken advantage of the vulnerability." Seemingly, Twitter's telemetry was insufficient to detect the malicious scraping.

Twitter is far from the first platform to expose data to mass scraping through an API flaw, and it is common in such scenarios for there to be confusion about how many distinct troves of data actually exist as a result of malicious exploitation. These incidents are still significant, though, because they add more connections and validation to the massive body of stolen data that already exists in the criminal ecosystem about users.

"Obviously, there are multiple people who were aware of this API vulnerability and multiple people who scraped it. Did different people scrape different things? How many troves are there? It kind of doesn't matter," says Troy Hunt, founder of the breach-tracking site HaveIBeenPwned. Hunt ingested the Twitter data set into HaveIBeenPwned and says that it represented information about more than 200 million accounts. Ninety-eight percent of the email addresses had already been exposed in past breaches recorded by HaveIBeenPwned. And Hunt says he sent notification emails to nearly 1,064,000 of his service's 4,400,000 million email subscribers.

"It's the first time I've sent a seven-figure email," he says. "Almost a quarter of my entire corpus of subscribers is really significant. But because so much of this was already out there, I don't think this is going to be an incident that has a long tail in terms of impact. But it may de-anonymize people. The thing

I'm more worried about is those individuals who wanted to maintain their privacy.”

Twitter wrote in August that it shared this concern about the potential for users' pseudonymous accounts to be linked to their real identities as a result of the API vulnerability.

“If you operate a pseudonymous Twitter account, we understand the risks an incident like this can introduce and deeply regret that this happened,” the company wrote. “To keep your identity as veiled as possible, we recommend not adding a publicly known phone number or email address to your Twitter account.”

See What's Next in Tech With the Fast Forward Newsletter

A weekly dispatch from the future by Will Knight, exploring AI advances and other technology set to change our lives. Delivered every Thursday.

Your email

Enter your email

SUBMIT



By signing up you agree to our [User Agreement](#) (including the [class action waiver and arbitration provisions](#)), our [Privacy Policy & Cookie Statement](#) and to receive marketing and account-related emails from WIRED. You can unsubscribe at any time.

For users who hadn't already linked their Twitter handles to burner email accounts at the time of the scraping, though, the advice comes too late. In August, the social network said it was notifying potentially impacted individuals about the situation. The company has not said whether it will do further notification in light of the hundreds of millions of exposed records.

Ireland's Data Protection Commission [said](#) last month that it is investigating the incident that produced the trove of 5.4 million users' email addresses and phone numbers. Twitter is also currently under

investigation by the US Federal Trade Commission over whether the company violated a “consent decree” that obligated Twitter to improve its user privacy and data protection measures.

Get More From WIRED

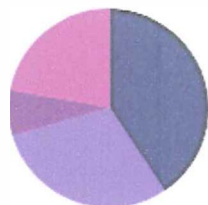
-  Don't miss [our biggest stories](#), delivered to your inbox every day
- The unbelievable zombie comeback of [analog computing](#)
- [Your next landlord](#) could be 100 random people
- Review: We put [ChatGPT, Bing Chat, and Bard](#) to the test
- The chemical menace inside [glaciers and icebergs](#)
- How a major toy company [kept 4chan online](#)
-  Our Gear team sounds off on [audiophile-grade speakers](#), [vinyl accessories](#) and the best [wireless headphones](#) for anyone



[Lily Hay Newman](#) is a senior writer at WIRED focused on information security, digital privacy, and hacking. She previously worked as a technology reporter at Slate magazine and was the staff writer for Future Tense, a publication and project of Slate, the New America Foundation, and Arizona State University. Additionally... [Read more](#)

SENIOR WRITER 

Data breaches for **davidsifuentes61@yahoo.com** ▾



Breached data

- Email addresses
- Passwords
- Phone numbers
- Other



2 of 5 emails monitored

[Manage emails](#)

11

Unresolved breaches

0

Resolved breaches

ANY

BREACHED DATA

DETECTED

Twitter (200M)

Email addresses

Active

01/05/2023

January 1, 2021, Twitter (200M) was breached. Once the breach was discovered and verified, it was added to our database on January 5, 2023. This breach exposed: Email addresses

Protect this breach:

Protect your email with an email masking service like [Firefox Relay](#).

Firefox Relay can hide your true email address while forwarding emails to your real inbox.



EXHIBIT C

For
Home

Products

Online Scan

Blog

Free Tools

Store

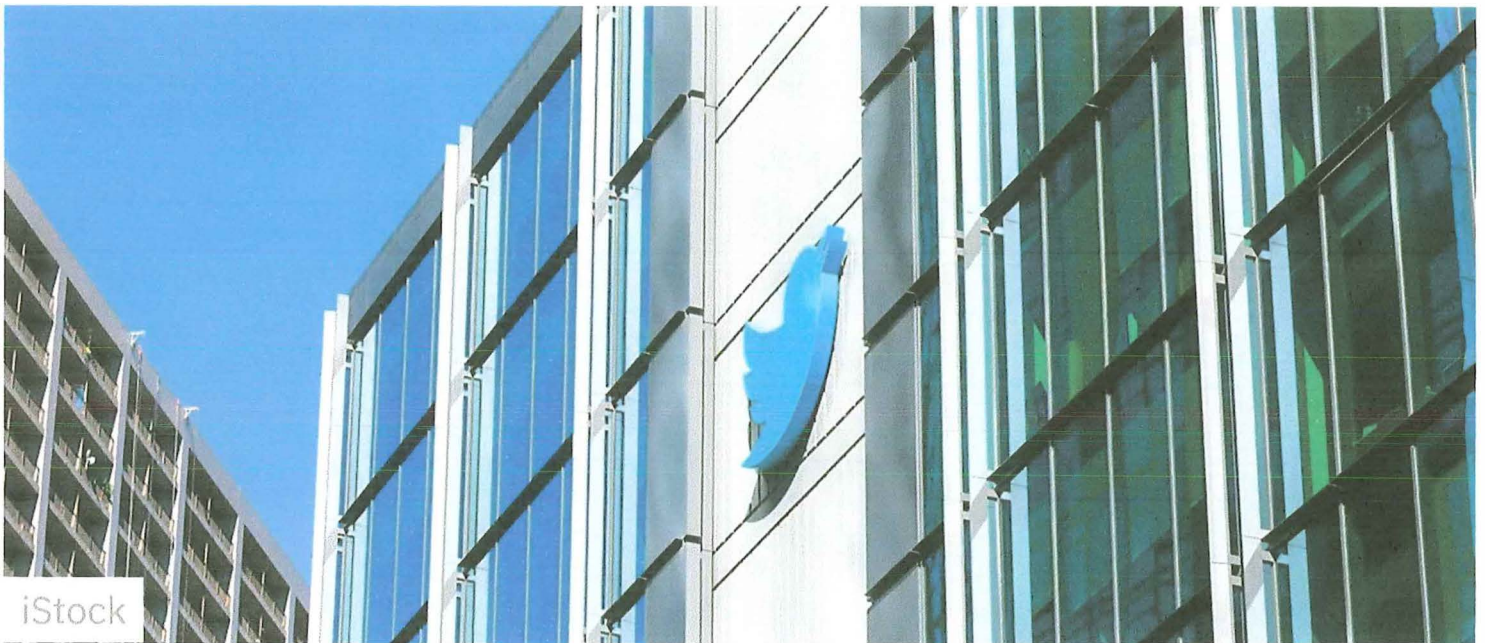
Support



Blog > Privacy

Twitter's January Data Leak Left 200 Million Users Exposed

February 24, 2023



The last year has been tough for social media giant Twitter, with volatility in the markets, new user **rules**, a **proliferation** of **scams**, and of course, **data leaks**. In fact, Twitter also started January with this year's first major data leak, in which a gigantic 200 million user email addresses were stolen and disseminated for free on hacker forums.

Twitter's January Data Leak

For Home

[Products](#)[Online Scan](#)[Blog](#)[Free Tools](#)[Store](#)[Support](#)

consisted of 59GB of data.

The **hack** used an existing Twitter **API vulnerability** to access email addresses and phone numbers; public data was then scraped to match these addresses/numbers to user accounts, enabling the hackers to create the Twitter profiles.

Email: [redacted]	- Name: Joe Osullivan - ScreenName: JoeOsullivan2 - Followers: 263 - Created At: [redacted]
Email: [redacted]	- Name: Pandora - ScreenName: FemaleWitticism - Followers: 68 - Created At: Sat Apr 21 [redacted]
Email: [redacted]	- Name: Eileen - ScreenName: EileenEmh66 - Followers: 3 - Created At: Thu Dec 19 12:3 [redacted]
Email: [redacted]	- Name: Sarah Thurlow - ScreenName: sjthurlow - Followers: 950 - Created [redacted]
Email: [redacted]	- Name: manishg4 - ScreenName: manishg4 - Followers: 332 - Created At: Sat Mar 21 17 [redacted]
Email: [redacted]	- Name: Victoria McIntyre - ScreenName: VictoriaMcInty1 - Followers: 3 - Cre [redacted]
Email: [redacted]	Name: amanda foster - ScreenName: mandyquinlivan - Followers: 0 - Created At [redacted]
Email: [redacted]	- Name: Roy Hughes - ScreenName: royjhughes - Followers: 3 - Created At: Sat [redacted]
Email: [redacted]	- Name: lesley stevens - ScreenName: lesleystevens55 - Followers: 5 - Creat [redacted]
Email: [redacted]	- Name: I'm Sooooo Confused - ScreenName: myConfusedLook - Followers: 0 - Crea [redacted]
Email: [redacted]	- Name: Rachael Carroll - ScreenName: rachaeloux - Followers: 0 - Created At: Mon [redacted]

Source: Bleeping Computer

Noted security expert and founder of Hudson Rock, Alon Gal, **stated**: “This is one of the most significant leaks I’ve seen ... [It] will unfortunately lead to a lot of hacking, targeted phishing, and doxxing.”

As investigations are ongoing, the controversy continues. While Twitter **claims** the leak was *not* due to a vulnerability in its systems, others disagree. At present, a large lawsuit is currently ongoing in California, with the legal challenge **stating**:


“At no point does Twitter disclose in their Privacy Policy that they allow cybercriminals to commandeer Twitter’s API in order to scrape sensitive PII from Twitter and to then weaponize or sell that information on the dark web ... [Twitter] buried its head in the sand.”

Was My Email Leaked and What Can I Do?

For Home

[Products](#)[Online Scan](#)[Blog](#)[Free Tools](#)[Store](#)[Support](#)

FREE Identity Protection platform (AKA “**idpanda**”), which has been specifically designed to meet these challenges.



What's leaked every month...

Category	Count
Email Addresses	2.4 billion
Phone Numbers	2.3 billion
Passwords	1.1 billion

Finding out if your personal data has been leaked can help you stay one step ahead of identity theft. Choose an option below to get started.

Email address [Check Now](#)

Your information is safe with us. Trend Micro doesn't store your data or sell it to third parties.

With Identity Protection, you can:

1. **Check** to see if your data (email, number, password, social media) has been exposed in a leak,
2. **Secure** your social media accounts with our Social Media Account Monitoring tool, with which you'll receive a personal report,
3. **Receive** the strongest tough-to-hack password suggestions from our advanced AI.